



IDACS QUARTERLY NEWS

Volume 2005, Issue 2
2nd Quarter 2005

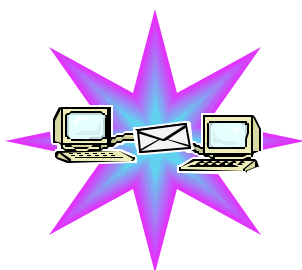
XAM Administrative Message

ISP System and Programming has recently completed another screen for AM Messages. This enhanced screen prompts the user with required fields that will fill in the NLETS required information.

The new required field of Message Number, ORI (Originating Agency Identifier), Destination ORN, Sending ORN, Send Date and Sent Time along with the Message Test Field when transmitted will

automatically form a properly structured NLETS AM Message.

This Enhance Administrative



Message (XAM) is located under the AM message in the IDACS drop down form menu. If field testing shows

positive remarks, this may become the only AM message choice within the next few months.

If an operator is unsure of what information to put into a field, right click the mouse, choose "FIELD HELP" and a help box will appear explaining the use of that field. The auto populated can be deleted and correct information inserted, if the auto populated information is inaccurate.

Inside this issue:

Reminders	2
Warrant Types	2
Disabled Veteran Plates	3
Validations	3
Directory Permissions	4

Can IDACS/NCIC INFORMATION BE E-MAILED?

System information is confidential, for law enforcement purposes only. Contents of an Email (which would include MDD, E-mail and MDD talk around) are a matter of public record. Therefore, by attaching system information to an email, you are assuming the respon-

sibility for a violation, should the public request these records. It is then a CJIS violation. Restricted data will include III/CHRI, BMV, all "Hot- file" etc. The system information can



be provided to employees through a Bulletin Board located in a secure area, printed copies in mailboxes, routers, etc...

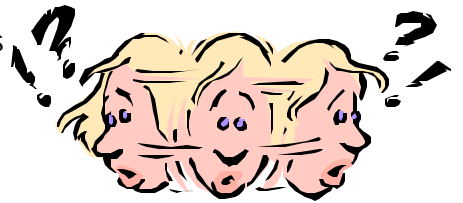
Remember, the only system information that can be provided to the public is Road and Weather.

Should you have any question feel free to contact the IDACS office at (317)232- 8292.

Reminders for Coordinators and operators

Operators: To keep from anyone accidentally or purposely using your USERID in Omnixx make sure your Password is personal and no one knows but yourself. If the challenge question you provided to IDACS has an answer that anyone can answer, then it will be very easy for anyone to call in as you and have your password changed. CHALLENGE QUESTIONS ARE VERY IMPORTANT TO YOUR OMNIXX LOG IN SAFETY. Also, if you are aware that you have two USER IDS within Omnixx, let your Coordinator know. Obtaining and using more than one USER ID is against IDACS Rules and Regulations.

Coordinators: If any operators are using or are assigned more than one USER ID, contact IDACS to have this issue resolved. User's are to only be using one (1) active USER ID. This is extremely important for the Audit Trail for each operator. In the event there are two USER ID's one will be disabled and the other will stay active.



All Coordinators now have the capability to view your operator's list. The CONSOLE ICON should be seen when you log onto Omnixx. If you are not able to view the CONSOLE ICON, contact IDACS to have that feature added for you.

When requesting USER IDS, make sure that you are using the correct format on the letterhead. There are 3 different types of certifications that can be given to a user; Full, Inquiry or MDD. Each operator must only have one certification. State on your request what level of certification the operator is to be given. If you need an example of how the request should be submitted, contact IDACS and a copy will be provided.

When requesting an IDACS Training class for users, the operator **MUST** have an assigned USER ID before they can attend. User's attending classes must be within 6 months before their certification is due to attend a class. If an operator is leaving your agency, submit a letter, fax or administrative message to the IDACS Section to have that user disabled. If the user is going to another agency, then submit that agency information on your request.

Wanted person file and the warrant type (wt y) field

In March 2004 the Warrant Type (WTY) field was added to the Wanted Person File. **This field will be marked "REQUIRED" on September 1, 2005.**

The WTY field along with the SSN of the wanted person will be forwarded to the Social Security Administration to help provide the wanting agency with last known addresses. This field will also provide statistical information in reference to the Wanted Person file.



If your agency does not use the Omnixx software and you would like to participate in the programs associated with the WTY field, your software vendor will need to add this field to your Wanted Persons entry screen. If you have any questions concerning this field, e-mail the IDACS section at Idacs@isp.state.in.us

Disabled veteran's plates

There are 5 different types of Disabled Veteran's Plates. Each license plate has a specific license type (LIT) in order to inquire on it. Below is a list of the different types of Disabled Veteran's Plates that are currently active. It also includes the LIT to be used and the issuing number by the BMV.

LIT	Name	class	% disabled	Issue #
DC	Disabled Veteran Motorcycle	2	100	1— 999
DM	Disabled Veteran Motorcycle	1	50	1— 854
DF	Disabled Veteran	1	100	1—9973
DH	Disabled Veteran	2	75	855—6000

An inquiry made on a regular Disabled Veteran Plate with no classification listed, the license type (LIT) will be DV. In the event that the above codes are not listed in the drop down code box, type the appropriate license type in the field and click on "transmit". If an "Error Box" is received, click on "Override" and the inquiry will be accepted.

Two (2) other license type (LIT) codes to be aware of are: LIT/HM for Disabled Motorcycle and LIT/HP for Handicap with the Wheelchair symbol on the license plate.



Terminal Agency Monthly Record Validation

On or about the 20th of the current month IDACS will send a message, over the system, advising the number and type of record(s) to be validated for the following month. The agency can retrieve the records to be validated by going to FORMS, then to IDACS, then to VALIDATIONS, and Request Validation Record Data (QVAD) form. All records must be validated by midnight of the last day of the month the record is due to be validated.

Non-terminal Agency Record Validation

On or about the 20th of the current month IDACS will send a message, over the system. The non-terminal agency records that are to be validated, for the following month, are electronically sent via the system to the terminal agency that provides service to that non-terminal agency

It is the responsibility of the terminal agency coordinator to see that the non-terminal agency receives a copy of those records to be validated.



Records still to be Validated

It is recommended that a QVAL (summary of records to be validated) be ran on or about the 25th of the month, to make sure that all of the records for the current month are validated, cleared, or canceled. This will let you know if there is records still to be validated. This will include the non-terminal agencies that the terminal agency provides service to, if any.

NOTE: There should not be any records purged due to non-

valida-





Accessing OMNIXX ... Do You Have Permission?

Though not strictly a concern of the CJIS ISO function, a particular aspect of local agency security frequently becomes a snare to the everyday user of the system, and of Omnixx in particular. Therefore, in this issue we will discuss the subject of "directory permissions" on the local Omnixx workstation, what they are, how they can affect you, and how to correctly set them.

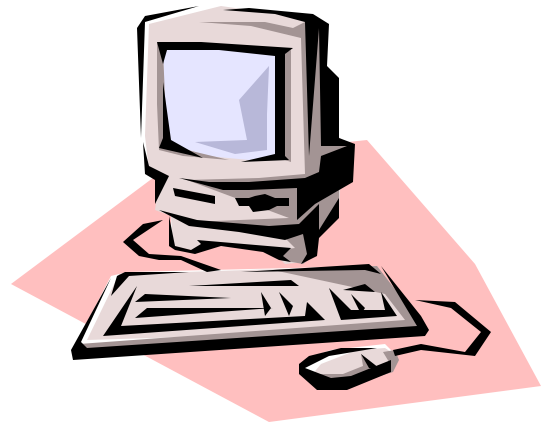
Directory permissions are security settings that control who can access the contents of folders on a workstation, and what they can do with those contents. Directory permissions include Full Control, Modify, Read & Execute, List Folder Contents, Read, and Write. Each of these permissions consists of a logical group of special permissions. The following table lists each folder permission and specifies which special permissions are associated with that permission.

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents	Read	Write
Traverse Folder / Execute File	x	x	x	x		
List Folder / Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files / Write Data	x	x				x
Create Folders / Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x			x	
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Accessing Omnixx (con)

Although List Folder Contents and Read & Execute appear to have the same special permissions, these permissions are inherited differently. List Folder Contents is inherited by folders but not files, and it should only appear when you view folder permissions. Read & Execute is inherited by both files and folders and is always present when you view file or folder permissions.¹

Directory permissions can be set for an individual user or for a group of users with common needs. Best practices for directory security are to keep users in groups defined by their common needs, and give only the groups permission to directories. Additionally, it is best to define permissions on top-level directories, and let those permissions directories underneath inherit permissions from the directories above. These practices reduce the number of permissions that must be maintained and prevent overlapping exceptions from creating holes in the security of the workstation.

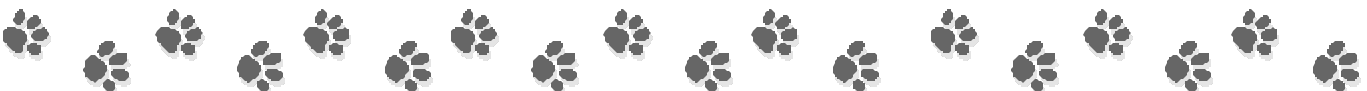


However, exceptions are occasionally required because of the unique requirements of a particular application. Omnixx is one such application. Because of the need to periodically download updates both to the transaction forms and message definitions, which are stored in the C:\OMNIXX directory, and to the core application Java components, which are stored in the C:\PROGRAM FILES\JAVA WEB START directory, permissions on these directories need to be broader than would otherwise typically be prudent. Insufficient directory permissions on these directories can result in anomalous behaviours ranging from a complete inability to launch Omnixx to a mystifying persistence of an old form when a new version is known to be available.

For Omnixx to function properly, the directory permissions for these folders should allow the user at least "Modify" permission, although in some circumstances "Full Control" permissions may need to be granted. This is not quite ideal, as it opens the possibility for someone to come along and *delete* the folder, including all of the audit logs; therefore, caution should be exercised before granting Full Control.

Adjustment to directory permissions requires a user with "Administrator" rights to the local workstation. For security reasons, actual procedures for changing these permissions will not be detailed in this space; but for more assistance with this, please have your technical specialist contact the IDACS Section.

¹ Preceding two paragraphs and table adapted from *Windows 2000 Professional Help: Folder Permissions*.



IDACS

Indiana State Police
IDACS Section
IGCN—100 N. Senate Ave.
Indianapolis, IN 46204-2259

Phone: 317-232-8292
Fax: 317-233-3057
Email: idacs@isp.state.in.us

We are on the web!
www.in.gov/isp/idacs

HOW TO TELL A WINNER FROM A LOSER

A winner says, "Let's find out"; a loser says, "Nobody knows."

When a winner makes a mistake, he says, "I was wrong"; when a loser makes a mistake, he says, "It wasn't my fault."

A winner goes through a problem; a loser goes around it, and never gets past it.

A winner makes commitments; a loser makes promises.

A winner says, "I'm good, but not as good as I ought to be; a loser says, "I'm not as bad as a lot of other people."

A winner tries to learn from those who are superior to him; a loser tries to tear down those who are superior to him.

A winner says, "There ought to be a better way to do it; a loser says, "That's the way it's always been done here."

Everybody loves a Winner!!

Unknown

IDACS STAFF

IDACS System Coordinator

Michael Dearing

Program Director

Andre' Clark

Administration

Holly White (Working Leader)

Sara Bloemker

IDACS Training

Kelly Dignin

Vivian Nowaczewski

Troy Scott

IDACS Security

Sgt. John Clawson

Sgt. John Richards



Data Operations Center Staff

Supervisor

Carrie Hampton

Day Shift (0700-1500)

Brian Thayer (Working Leader)

Ala Munn

LaJuan Harris (Working Leader)

Evening Shift (1500-2300)

Patsity Epps (Acting Working Leader)

Sheriff (Leldo Ba) Lee

Night Shift (2300-0700)

Fred Kline

Wayne Swift

